IN THE CLAIMS

1. (Currently amended) A method for enforcing restricted access of a media file, comprising:

storing a media file;

partitioning the media file into a plurality of sequential data blocks;

generating a plurality of cryptographic token keys;

encrypting the plurality of sequential data blocks with the plurality of cryptographic token keys, thereby producing a plurality of encrypted sequential data blocks;

transferring at least a subset of the plurality of encrypted sequential data blocks from a sending server to a receiving client;

selecting, by the sending server, a subset of the plurality of cryptographic token keys for transfer to the receiving client, wherein the subset of the plurality of cryptographic token keys enables decryption of one of more corresponding encrypted sequential data blocks of the transferred subset of the plurality of encrypted sequential data blocks, thereby enabling the receiving client to access only a selected portion of the media file as defined by the sending server, in accordance with an access status of the receiving client, and wherein the subset of the plurality of cryptographic token keys comprises fewer cryptographic token keys than the plurality of cryptographic token keys; and

transferring the subset of the plurality of cryptographic token keys from the sending server to the receiving client, wherein non-selected cryptographic token keys are not transferred to the receiving client as defined by the sending server, in accordance with the access status of the receiving client.

2. (Original) The method of claim 1, wherein the media file is a multimedia file.

3. (Original) The method of claim 1, wherein the media file is a video file.

4. (Original) The method of claim 1, wherein the media file is an audio file.

5. (Original) The method of claim 1, wherein the media file is a text file.

6. (Original) The method of claim 1, wherein the media file contains a time-sequential presentation which can be perceived by one or more of the senses.

7. (Original) The method of claim 1, wherein said partitioning further comprises:

compressing selected ones of the plurality of sequential data blocks.

8. (Original) The method of claim 1, wherein said generating further comprises:

generating one cryptographic token key for each one of the plurality of sequential data blocks.

9. (Original) The method of claim 8, wherein said encrypting further comprises:

encrypting each one of the plurality of sequential data blocks with a corresponding one of the plurality of cryptographic token keys.

10. (Original) The method of claim 1, wherein said transferring further comprises:

recording the encrypted sequential data blocks on a recording medium.

11. (Previously presented) The method of claim 1, wherein said transferring of at least a subset of the plurality of encrypted sequential data blocks further comprises:

transmitting over a communications link at least the subset of the plurality of encrypted sequential data blocks.

12. (Previously presented) The method of claim 1, wherein said transferring of the subset of the plurality of cryptographic token keys further comprises:

transmitting over a communications link the subset of the plurality of cryptographic token keys.

13. (Previously presented) The method of claim 12, which further comprises:

transmitting the subset of the plurality of cryptographic token keys in a sequence corresponding to a predetermined order of decryption of the one or more corresponding encrypted sequential data blocks of the transferred subset of the plurality of encrypted sequential data blocks.

14. (Previously presented) The method of claim 12, which further comprises:

transmitting the subset of the cryptographic token keys in a token block, wherein each respective cryptographic token key may be retrieved from the token block in a sequence ordered by an order of occurrence decryption of the one or more corresponding encrypted sequential data blocks of the transferred subset of the plurality of encrypted sequential data blocks.

15. (Previously presented) The method of claim 1, which further comprises:

sequentially decrypting at the receiving client, each of the one or more corresponding encrypted sequential data blocks of the transferred subset of the plurality of encrypted sequential data blocks using a corresponding one of the subset of plurality of cryptographic token keys, thereby recovering and providing access to the selected portion of the media file.

16. (Previously presented) The method of claim 12, which further comprises:

streaming each of the subset of cryptographic token keys in a sequence ordered by an order of occurrence of decryption of the one or more corresponding encrypted sequential data blocks of the transferred subset of the plurality of encrypted sequential data blocks.

17. (Currently amended) A system for enforcing restricted access of a media file, comprising:

a server for storing a media file;

a program in the server for partitioning the media file into a plurality of sequential data blocks;

a program in the server for generating a plurality of cryptographic token keys;

a program in the server for encrypting the plurality of sequential data blocks with the plurality of cryptographic token keys, thereby producing a plurality of encrypted sequential data blocks;

a program in the server for transferring at least a subset of the plurality of encrypted sequential data blocks from the server to a receiving client;

a program in the server for selecting a subset of the plurality of cryptographic token keys for transfer to the receiving client, wherein the subset of the plurality of cryptographic token keys enables decryption of one or more corresponding encrypted segmented data blocks of the transferred subset of the plurality of encrypted sequential data blocks, thereby enabling the receiving client to access only a selected portion of the media file as defined by the server, in accordance with an access status of the receiving client, and wherein the subset of the plurality of cryptographic token keys comprises fewer cryptographic token keys than the plurality of cryptographic token keys and

a program in the server for transferring the subset of the plurality of cryptographic token keys from the server to the receiving client, wherein the non-selected cryptographic token keys are not transferred to the receiving client as defined by the sending server, in accordance with an access status of the receiving client.

18. (Canceled)

19. (Currently amended) A computer program product for enforcing restricted access of a media file, comprising:

a computer readable medium;

a computer program code for partitioning a media file into a plurality of sequential data blocks;

a computer program code in said computer readable medium for generating a plurality of cryptographic token keys;

a computer program code in said computer readable medium for encrypting the plurality of sequential data blocks with the plurality of cryptographic token keys, thereby producing a plurality of encrypted sequential data blocks;

a computer program code in said computer readable medium for transferring at least a subset of the plurality of encrypted sequential data blocks from a sending server to a receiving client;

a computer program code in said computer readable medium for selecting a subset of the plurality of cryptographic token keys for transfer to the receiving client, wherein the subset of the plurality of cryptographic token keys enables decryption of one or more corresponding encrypted sequential blocks of the transferred subset of the plurality of encrypted sequential data blocks, thereby enabling the receiving client to access only a selected portion of the media file as defined by the sending server, in accordance with an access status of the receiving client, and wherein the subset of the plurality of cryptographic token keys comprises fewer cryptographic token keys than the plurality of cryptographic token keys; and

a computer program code in said computer readable medium for transferring the subset of the plurality of cryptographic token keys from the sending server to the receiving; client, wherein the non-selected cryptographic token keys are not transferred to the receiving client as defined by the sending server, in accordance with an access status of the receiving client.